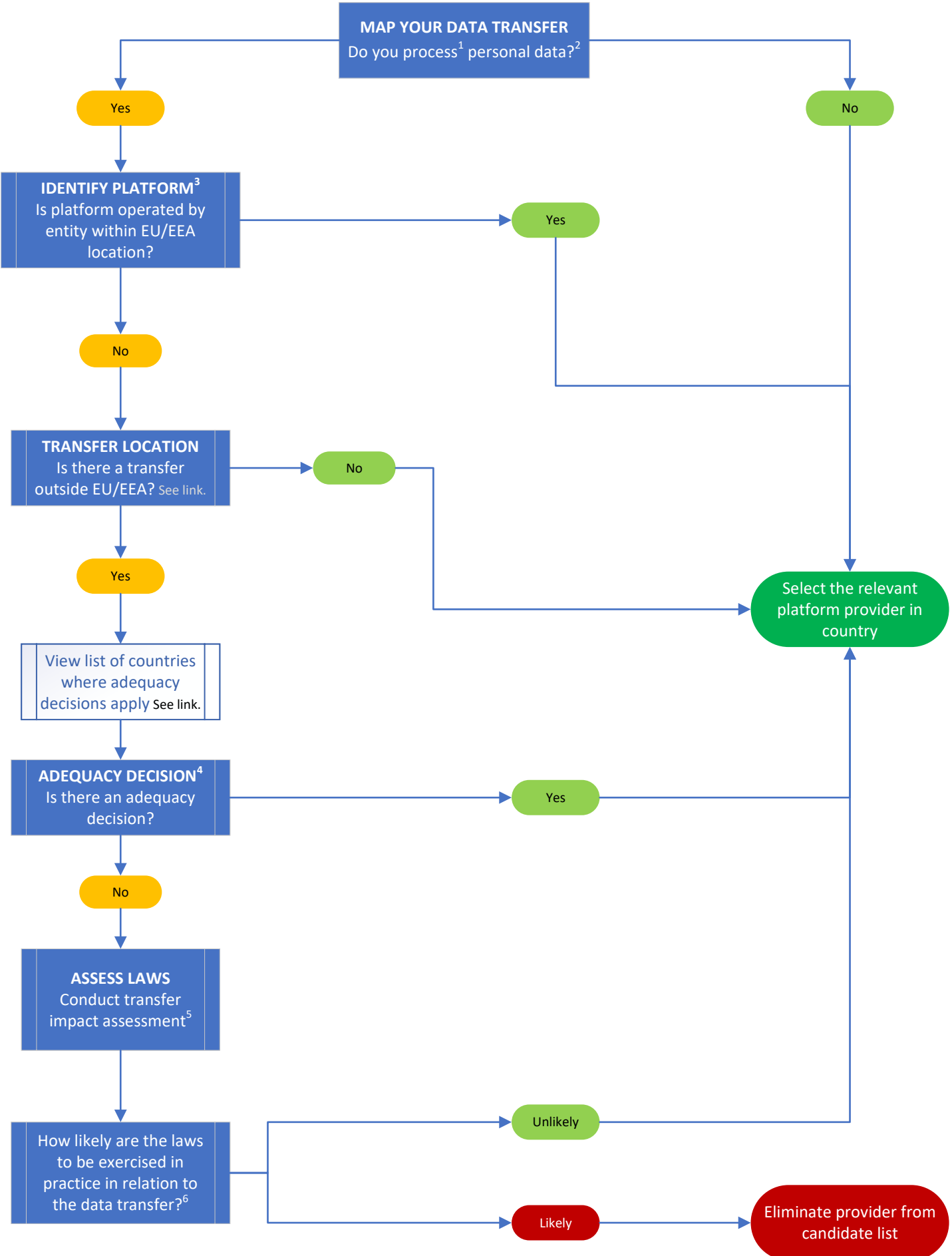


GDPR Transfer Guide
for
National Research and Education Networks (NRENs)
on the
2020 IaaS+ Framework

The following document is intended for use by NRENs seeking to use,
or actively using, the 2020 IaaS+ Framework.

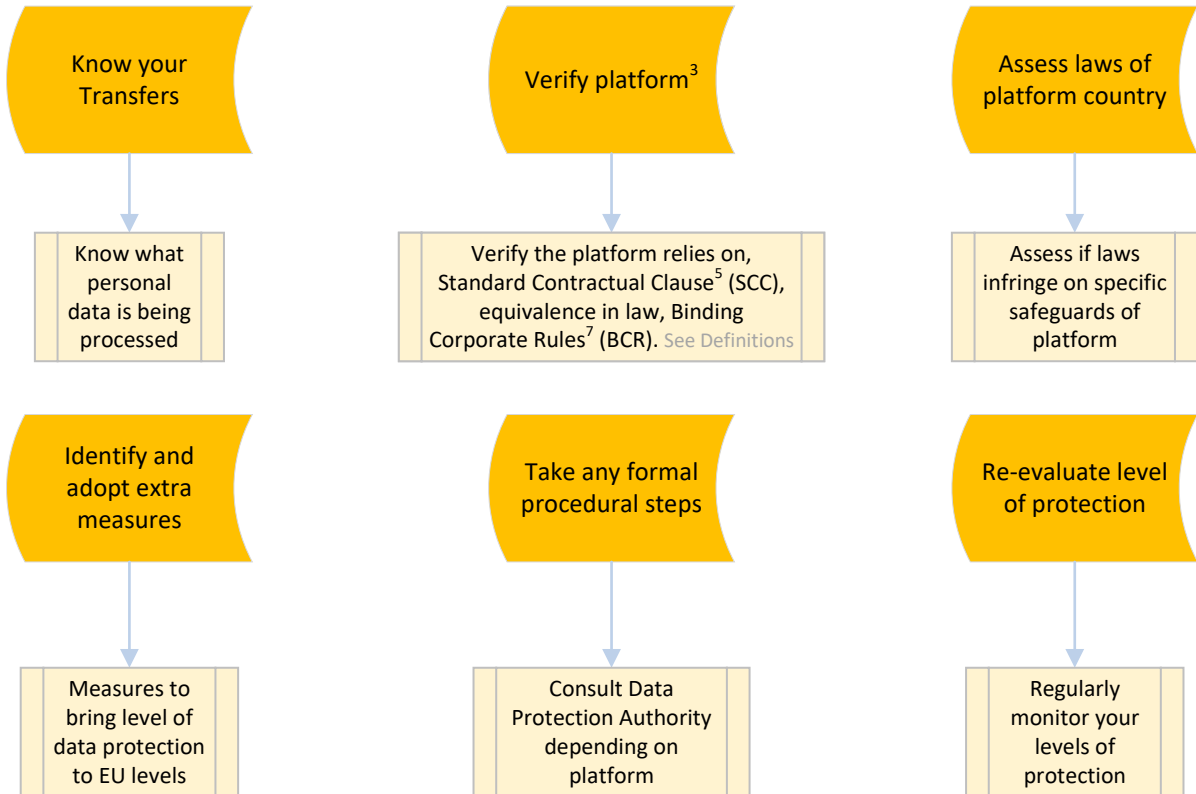
The information contained in this document is intended as guidance but does not
constitute legal advice.

Personal Data Transfer Checklist



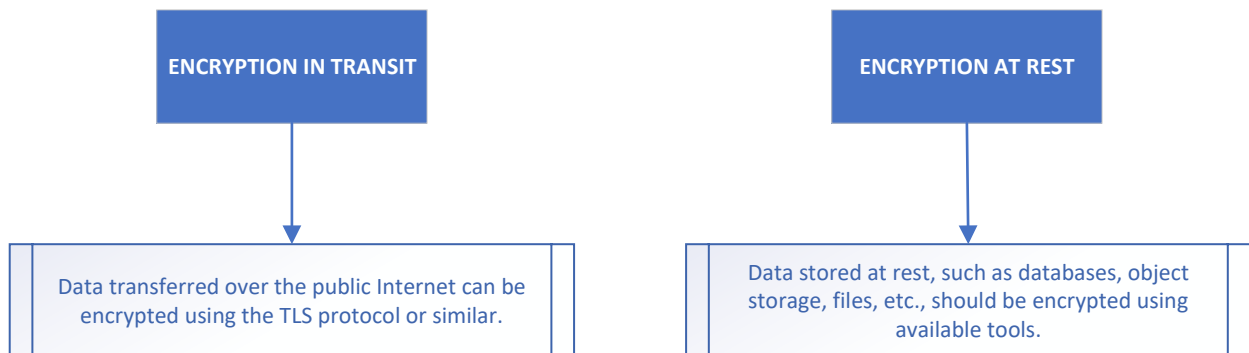
Data Transfer Checklist

Some, or all, of the below steps apply to all platforms regardless of where the platform resides



Data Encryption Options

Below are some considerations in relation to data encryption and how it may impact on use of cloud services.

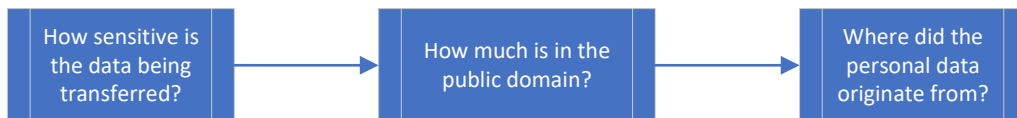


Transfer Impact Assessment (TIA)

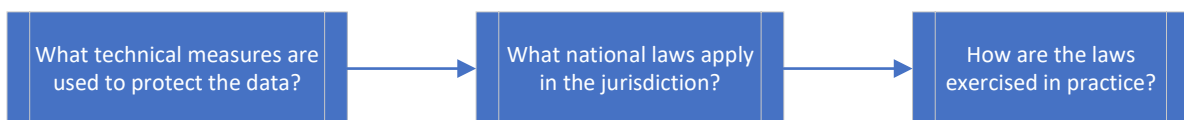
This is a flexible risk assessment which needs to be monitored regularly and updated in light of changes in laws

THE DATA

WHAT PERSONAL DATA IS BEING TRANSFERRED?



THE LAWS



THE RESULT OF THE TIA

How likely are they to be exercised in relation to the platform?

Definitions

1. **Process(ing)** – any operation or set of operations performed on personal data.
2. **Personal data** – any information which is related to an identified or identifiable natural person.
3. **Platform** – some documentation may refer to Transfer Tool. In this instance this is the platform.
4. **Adequacy decision**
There is an adequacy decision for countries like the UK, Switzerland, Argentina, Japan, etc. More information and the full list of countries can be found [here](#).
5. **Transfer impact assessment (TIA)**
 - Questionnaire to be completed by either party to the data transfer i.e. data importer or data exporter.
 - Clarifies organisation's risks for transferring EU residents' data to countries without adequacy under GDPR.
 - The TIA will be executed together with the Standard Contractual Clauses. Further information can be found [here](#).
6. For FISA, or similar, check if the perceived risk is higher than the threat of data theft by a malicious actor, including state sponsored data theft. If so consider:
 - a) applying your existing risk mitigation strategies to protect against data theft and/or,
 - b) bring Your Own Encryption Key and/or,
 - c) if Binding Corporate Rules and Standard Contractual Clauses mitigate the perceived risk and/or,
 - d) if there are improvements in the platform coming that can further reduce perceived risk
7. For more information on Binding Corporate Rules BCR click [here](#).